Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft's April 2025 Patch Tuesday Fixes Active Zero-Day Exploits

Date of Publication	Admiralty Code	TA Number
April 9, 2025	A1	TA2025106

Summary

First Seen: April 9, 2025
Affected Platforms: Microsoft Windows, Microsoft Office, Microsoft Windows LDAP, Microsoft SharePoint and more
Impact: Elevation of Privilege, Denial of Service, Information Disclosure, Remote Code Execution, Spoofing, Security Feature Bypass
Actor: Storm-2460
Malware: PipeMagic

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-29824	Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2025-26663	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-26670	Lightweight Directory Access Protocol (LDAP) Client Remote Code Execution Vulnerability	Microsoft Windows LDAP	✗	✗	✓
CVE-2025-27472	Windows Mark of the Web Security Feature Bypass Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-27480	Windows Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2025-27482	Windows Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-27727	Windows Installer Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-29792	Microsoft Office Elevation of Privilege Vulnerability	Microsoft Office	✗	✗	✓
CVE-2025-29793	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	✗	✗	✓
CVE-2025-29794	Microsoft SharePoint Remote Code Execution Vulnerability	Microsoft SharePoint	✗	✗	✓
CVE-2025-29809	Windows Kerberos Security Feature Bypass Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2025-29812	DirectX Graphics Kernel Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓

Vulnerability Details

#1

Microsoft's April 2025 Patch Tuesday includes security updates for 126 vulnerabilities, classified as 11 critical, 112 important, and 2 Low severity vulnerabilities. These encompass 33 Remote Code Execution, 49 Elevation of Privilege, 17 Information Disclosure, 14 Denial of Service, 9 Security Feature Bypass, and 3 Spoofing vulnerabilities. One CVE (CVE-2025-29817) appears to be reserved and lacks detailed information, resulting in a total count of 125 CVEs.

#2

The updates apply to a broad range of Microsoft products, including Windows, Office, Visual Studio, Windows Remote Desktop Services, Windows Hyper-V, Microsoft Management Console, and other components. Notably, Microsoft also addressed nine Chromium-assigned vulnerabilities affecting the Chromium-based Microsoft Edge browser, bringing the total number of patched CVEs to 134. This advisory addresses 12 CVEs with potential exploitation risks.

#3

The report addresses one actively exploited zero-day vulnerability along with multiple critical remote code execution (RCE) flaws. The zero-day, CVE-2025-29824 is a Use-After-Free vulnerability in the Windows Common Log File System (CLFS) driver. This flaw is being actively exploited in the wild to achieve local privilege escalation. It has been linked to the PipeMagic malware, which has been deployed in targeted attacks attributed to Storm-2460, a threat actor also known for using the same malware to distribute ransomware. This zero-day highlights the increasing use of privilege escalation bugs as a steppingstone for full system compromise.

#4

Among the patched vulnerabilities are two critical flaws CVE-2025-26663 and CVE-2025-26670 impacting Windows LDAP and LDAP Client, respectively. Both stem from race conditions that lead to Use-After-Free scenarios, enabling attackers to remotely execute arbitrary code by sending specially crafted requests. Successful exploitation could allow an attacker to take control of affected systems, making these bugs especially concerning for enterprise environments.

#5

The update also resolves CVE-2025-27480 and CVE-2025-27482, two RCE vulnerabilities in Windows Remote Desktop Gateway Service. These issues are triggered by race conditions and require no user interaction to exploit, significantly raising the risk for internet-facing RDP deployments. Attackers capable of winning the race condition can gain full control over the target system without needing to trick the user.

#6

Finally, Microsoft SharePoint Server receives important fixes for CVE-2025-29793 and CVE-2025-29794. These RCE vulnerabilities are remotely exploitable over the internet and rated with low attack complexity, meaning attackers can achieve repeatable success without deep system knowledge. Their exposure to internet-based attacks makes them a top concern for organizations running SharePoint in production.

#7

With threat actors already leveraging these flaws in the wild, staying up to date is essential to minimizing risk and protecting systems from compromise. These vulnerabilities underscore the importance of applying the April 2025 patches to protect against potential exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-29824	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-26663	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-26670	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-416

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-27472	Windows: 10 Windows Server: 2012	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-693
CVE-2025-27480	Windows Server: 2012 - 2025	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-27482	Windows Server: 2016 - 2025	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-591
CVE-2025-27727	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-59
CVE-2025-29792	Microsoft Office: 2016 - 2024	cpe:2.3:o:microsoft:office:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-29793	Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	cpe:2.3:o:microsoft:sharepoint_server:*:*:*:*:*:*:*:*:*	CWE-502
CVE-2025-29794	Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	cpe:2.3:o:microsoft:sharepoint_server:*:*:*:*:*:*:*:*:*	CWE-285

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-29809	Windows: 10 - 11 24H2 Windows Server: 2016 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-922
CVE-2025-29812	Windows: 11 24H2 Windows Server: 2022 - 2025	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-822

Recommendations

- Conduct an extensive service exposure evaluation to identify any vulnerable services that may be publicly accessible. Take immediate and decisive action to address any identified vulnerabilities, either by installing essential **patches** or adopting security measures.
- Keep your systems up to date by implementing the most recent security updates. To avoid the introduction of new vulnerabilities, follow security rules adapted to unique devices. Furthermore, to strengthen the resilience of devices and apps exposed to the internet, thoroughly review their configurations.
- Prioritize patching the actively exploited vulnerability CVE-2025-29824. This vulnerability pose significant exploitation risks and should be addressed urgently.
- Implement network segmentation to restrict unauthorized access and reduce the impact of potential attacks. This can be especially effective in scenarios where network adjacency is a factor.
- Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	T1588 Obtain Capabilities	T1588.005 Exploits
T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation	T1133 External Remote Services
T1553 Subvert Trust Controls	T1553.005 Mark-of-the-Web Bypass	T1566 Phishing	T1204 User Execution
T1204.002 Malicious File	T1204.001 Malicious Link	T1558 Steal or Forge Kerberos Tickets	

Indicator of Compromise (IOCs)

TYPE	VALUE
File Path	C:\ProgramData\SkyPDF\PDUDrv.blf, C:\Windows\system32\dllhost.exe –do
Domain	aaaaabbbbbbb[.]eastus[.]cloudapp[.]azure[.]com
TOR Address	jbdg4buq6jd7ed3rd6cynqtq5abttuekjnxqrqyvk4xam5i7ld33jvqd[.]onion, uyhi3ypdkfeymyf5v35pbk3pz7st3zamsbjzf47jiqbcm3zmikpwf3qd[.]onion

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26663

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26670

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27472

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27480

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27482

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27727

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29792

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29793

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29794

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29809

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29812

References

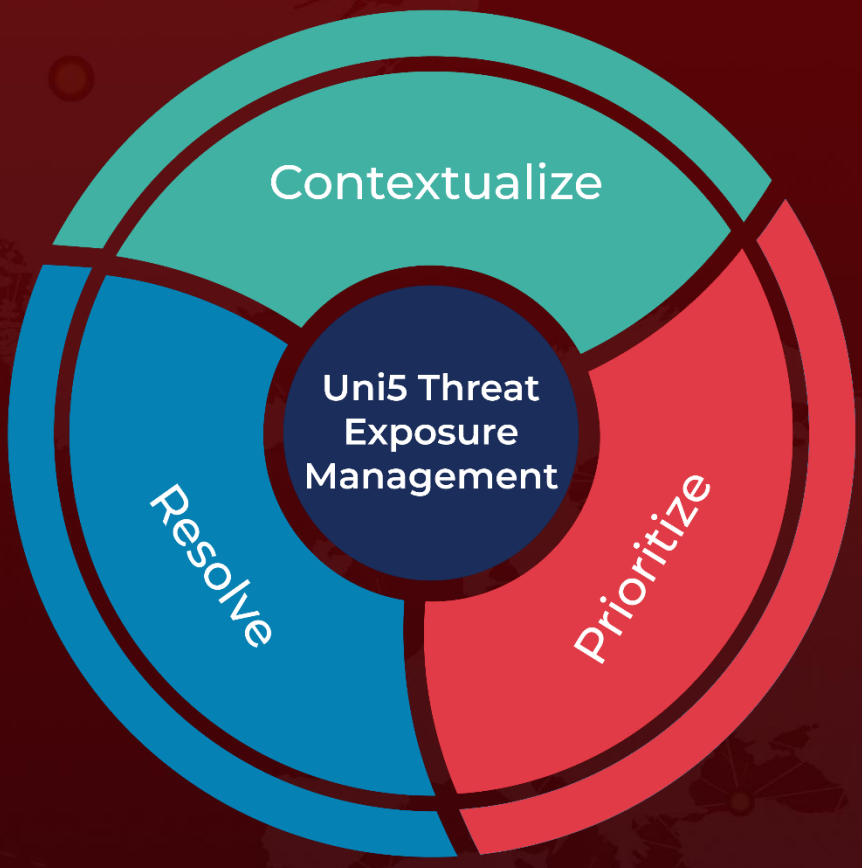
https://msrc.microsoft.com/update-guide/releaseNote/2025-apr

https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 9, 2025 • 8:40 AM

More at www.hivepro.com